# TABULAR MAPPING OF STAKEHOLDERS' RESPONSES TO THE WHITE PAPER ON A DATA PROTECTION FRAMEWORK FOR INDIA

## PART III – GROUNDS OF PROCESSING

The following table was prepared after an analysis of all twenty-seven (27) responses to questions in chapters 1, 2, 3 and 4 of Part III to the White Paper on a Data Protection Framework for India: - Should consent be a primary ground for processing personal data? Should the proposed law have a provision prescribing an age-bar specifically for protecting children's personal data? Should the law rely on the notice and choice mechanism for operationalising consent? What are the other grounds that may be considered for permissible processing of personal data?

The table identifies the responses and suggestions of the stakeholders to the questions.

| **Stakeholders** | | **Consent should be a primary ground for processing personal data** | **Child's consent and provision prescribing an age-bar specifically for protecting children's personal data in the proposed law** | **The law should rely on the notice and choice mechanism for operationalizing consent** | **Any other grounds of processing data** |
|---|---|---|---|---|---|
| **Industry Associations –3*** <br><br> BSA, iSPIRT, and ITI | BSA | Consent is important for handling personal data. However, it is suggested that government should recognize legal bases for processing personal | An age limit of 13, which is incorporated into US law, and is also the lower threshold under the EU GDPR is | When express consent is required, a clear and conspicuous notice that provides individuals with information relevant to their choice | There should be multiple grounds for processing personal data such as:- 1) Legitimate interest, 2) compliance with legal obligations |

| | | | | | |
|---|---|---|---|---|---|
| | | data. Legal bases such as legitimate interest of companies handling the data, the performance of contracts with the data subject, and compliance with legal obligations should be incorporated in the law. | suggested to be adopted in the Indian data protection framework. | should be provided. | such as financial reporting rules, other regulatory requirements, and obligations arising from court proceedings, and 3) Contractual performances. |
| | iSPIRT | Consent should be the primary ground of processing personal data. | A child's consent is not valid. Consent needs to be from a responsible adult. | Law should rely on notice and choice mechanism for operationalising consent. Government data controller should use a specific language and standardize the notices. | The grounds for processing which are necessary other than consent are:-<br>1) Compliance with the law 2) Performance of contract (with the individual) 3) Emergency situation/ vital interest. |
| | ITI | Consent should be collected in a manner which serves both the purposes i.e. right of individuals to control their personal data, and their own need to collect, use or disclose it. | India should adopt provisions similar to EU, where the age of consent for children is set at 13. It shall bring more consistency across legal regimes. | No response | It is suggested that India should adopt policies that are similar to EU GDPR where processing should be done for legitimate interests of data controllers, such as 1) direct marketing purposes or preventing fraud; 2) transmission of |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | personal data within a group of undertakings for internal administrative purposes, including client and employee data; 3) purposes of ensuring network and information security, including preventing unauthorized access to electronic communications networks and stopping damage to computer and electronic communication systems; and 4) reporting possible criminal acts or threats to public security to a competent authority. |
| **Civil society organisations – 12****<br><br>Access Now; CCG; CIS; Centre for | Access Now | "Implied consent" contradicts the objective of putting the user in control of their personal data as they might not be fully aware of the fact that their information will be | No response | Individuals should be provided with notices when there is threat to their privacy. For informed consent, proper notices are essential. | Processing of personal data based on legitimate interest of companies shouldn't be authorised without strict limitations. |

| | | | | | |
|---|---|---|---|---|---|
| Trade and Investment Law; Harvard FXB Center; IDP; Mozilla Foundation; ORF; Professor Graham Greenleaf; SFLC; Legal Academics and Advocates; Takshashila Institution. | | processed. Consent should be an affirmative action. | | | |
| | CCG | No response | No response | No response | No response |
| | CIS | Consent should be freely given. India should incorporate the provisions of the GDPR which clarifies when the consent is not freely given. It is considered not freely given, when the data subject has no genuine and free choice or is unable to refuse or withdraw consent without detriment (Recital 42); and/or there is a clear imbalance between the data subject and the controller (Recital 4). | The digital age of consent for children can be grouped as:<br>1. Below 13 years (consent to be given only by parent or legal guardian);<br>2. 13 - 18 years (or possibly 16 years – with parental consent) and<br>3. Above 18 (consent of the user is sufficient). | The privacy notices should include the following information:<br>1. What personal information is being collected;<br>2. Name and contact details of the entity collecting the data;<br>3. Purposes for which personal information is being collected;<br>4. Uses of collected personal information;<br>5. Whether or not personal information may be disclosed to | The other grounds of processing should be:<br>1. Vital interest - This ground may be used only in limited circumstances, such as where there is a threat to the life or health of the individual;2. Performance of contract – there can be two grounds for performance of contracts. Firstly, where processing is necessary for the performance of a contract to which the data |

| | | | | | |
|---|---|---|---|---|---|
| | | | | third persons, and the third party recipients or categories of recipients of the personal data;<br>6. The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;<br>7. The manner in which it may be accessed, verified and modified;<br>8. The procedure for recourse in case of any grievance in relation to collection and processing of data;<br>9. Security safeguards | subject is a party, secondly, where it is intended to cover any processing activity, which could take place prior to entering a contract. This includes pre contractual relations. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | established by the data controller in relation to the personal information;<br>10. Contact details of the privacy officers and ombudsman for filing complaints. | |
| | Centre for Trade and Investment Law | No response | No response | No response | No response |
| | Harvard FXB Center | Clinical care and research will be negatively affected if consent to access health data becomes difficult. It is, therefore, suggested that a set standard for consent should be applied across the private and public healthcare delivery organizations. Consent for health data may be implicit when it fulfils | Processing of children's health data, for purposes outside a legal or contractual obligation, may need stricter scrutiny and consent. Restrictions should not preclude children and adolescents from accessing health information or health services in privacy, | For health data, notice is important, but cannot be the only mechanism for operationalizing consent. Notice in form of audio visual should be provided to those with poor literacy. When an individual is unable to understand the notice, the law should provide for opt-ins instead of opt-outs. However, as far as | The other grounds necessary for processing are as follows:<br>1. Performance of contract;<br>2. Legal obligations;<br>3. Vital Interest such as protecting life of another individual;<br>4. Public Interest Task, Exercise |

| | | | | | |
|---|---|---|---|---|---|
| | | criteria like legal or contractual obligation. Consent for health data needs to be unambiguous when the data are identifiable. EU GDPR guidelines should be applied in the Indian context, requiring consent to be meaningful and accessible. | especially services that affect sexual or behavioural health. | possible the architecture of the health data ecosystem is concerned, it should not rely on notice and choice. | of Official Authority;<br>5. Legitimate Interest. |
| | IDP | It is suggested that even if consent is one of the important factors in data processing, it has limited role to play in the data protection framework. Further, it is suggested that, consent should be:<br>1. Unbundled;<br>2. Unambiguous<br>3. Uncoerced;<br>4. Express and<br>5. Obligations to comply with proposed principles like privacy-by- | No response | 'Notice' is one of the global best practices as per the AP Shah Committee report. The list of heads in the above-mentioned report, for which notice is required, and its manner, remains relevant, including the requirement to notify individuals 'of any legal access to their personal information after the purposes of the access have been met'. Notice in cases of profiling should be added to this | No response |

| | | | | | |
|---|---|---|---|---|---|
| | | design, purpose limitation, should apply | | list. | |
| | Mozilla Foundation | Consent is an important aspect in data protection framework. However, some exception to a consent model may be advisable in the cases where the data collected is not personal. Consent is one of the first links of a security chain that includes, but is not limited to, additional links like privacy by design, storing and transmitting data securely, collection and purpose limitation, oversight by the data protection authority, data breach notification, etc. Of course, if the link of consent is weak or broken, the integrity of the rest of the chain is compromised. Consent must be meaningful. | No response | No response | Legitimate interest has been suggested as other ground for processing data. |
| | ORF | Informed and | No response | No response | No response |

| | | | | | |
|---|---|---|---|---|---|
| | | meaningful consent is the foundational protection in data collection. Consent must be freely and expressly obtained with purpose specification for collection, handling and transfer of data. Consent must be simplified and multilingual. Consent must also be flexible allowing users the option to revoke access to their personal information at a subsequent time. Every user must also have a right to retain a copy of his/her aggregated information and the right to erase copies of the information stored with the primary data controller. | | | |
| | Professor Graham Greenleaf | Other than the provisional views regarding consent, it is suggested that, consent should be 'unbundled', | Parental authorisation or consent should be obtained when data controllers process | Notice should be mandatory where information is collected from the data subject (GDPR, art.13), | The other grounds recommended are as follows:<br>1. Performance of contract; |

| | | | | | |
|---|---|---|---|---|---|
| | | or should be separated from other information, such as:<br>1. Separation of consent for each item requiring consent, not one overall consent (GDPR, art. 7(2)); and<br>2. Separation of consent from the collection of any other information not necessary for the performance of the contract (GDPR, art. 7(4)). | personal data relating to children. A variable age limit can be drawn (not necessarily 18- which is the generally accepted age of majority in India) below which parental consent is to be mandatory. | and where information is collected other than from the data subject (GDPR, art.14). | 2. Compliance with law;<br>3. Public interest;<br>4. Collection of information in situations of emergency where it may not be possible to seek consent from the affected individual. |
| | SFLC | Consent is an important ground for data processing, but relying on it solely is not sufficient. The objective of the law should be giving an individual control over | Under Section 11 of the Indian Contract Act, 1872, a minor is incapable of entering into a contract. Section 3 of the Indian Majority Act, 1875 sets the age of | The data protection law should prescribe for a method of notice and choice. It is a positive obligation on a data controller/processor as it creates a sense of awareness among the | The following can be recognized as other grounds of processing:<br>1. Where processing is necessary to perform a |

| | | | | | |
|---|---|---|---|---|---|
| | | his/her personal information. Consent should be an essential ground for processing when a data controller is collecting data from a data subject. It should however be complemented with other robust data protection principles to protect the individual from any potential harm. The following conditions can be applied to make consent more meaningful:<br>1. Consent must be explicit, specific, unambiguous, and freely given;<br>2. Consent must be informed: The data subject should know what exactly he/she is consenting to; | majority at 18 years. This age is perfectly acceptable for the purposes of data protection. There is no need of lowering the age limit. | data subjects and gives them a choice to part with their data. The notice should be simple and comprehensible. That can be achieved by employing the following methods:<br>1. Use of plain and simple language with clear fonts, no legalese and ;<br>2. Use of clear explanations of purpose and uses;<br>3. Use of regional languages apart from English to draft notices;<br>4. Use of standardized icons for activities such as profiling, data sharing, collection of sensitive personal data, | contract that the data subject has consented to;<br>2. In order to protect the data subject's vital interests i.e in an emergency situation, for e.g. where a medical condition may be disclosed to treat the data subject; |

| | | | | | |
|---|---|---|---|---|---|
| | | 3. The data subject should have the right to withdraw consent during any stage of processing. | | withdrawal of consent (delete my data) and grievance redressal; and<br>5. Graphical assistance capable of explaining terms and conditions to consumers. | |
| | Legal Academics and Advocates | Consent and notice shall be vital to any data protection regulation. User centric principles such as choice and consent, should not be used to transfer organisation's privacy obligations to data subjects, instead the organisation should take responsibility for protecting privacy. | No response | A data controller should give simple-to-understand notice of its practices to all individuals, in clear and concise language, before any personal information is collected from them. The individuals should be informed of how their information shall be used, the intentions and practices of the data controllers should be communicated to data subjects and other | No response |

| | | | | | |
|---|---|---|---|---|---|
| | | | | stakeholders. | |
| | Takshashila Institution | Over-reliance on consent creates unnecessary burden on organisations and individuals without adding privacy protections. Therefore India should rely on the 'Accountability model' as the primary means for securing privacy. | There must be an absolute prohibition on the processing of Sensitive Personal Data of all children who have not attained the age of 14. In case of Sensitive Personal Data and Identified Personal Data of children above 14, explicit parental consent should be the foundation for processing. | Individuals should be informed about the collection and use of their personal information so that they make more informed decisions about how their information may be used. Notice is not required where the personal data should remain confidential subject to an obligation of professional secrecy regulated by law, including a statutory obligation of secrecy. | Four other grounds of processing are suggested. They are:-<br>1. Performance of contract;<br>2. Public Interest;<br>3. Vital interest of subject;<br>4. Legitimate interest of the controller. |
| **Others-12*** **<br><br>Anupam Saraph; Bhandari, Kak, Parsheera, Rahman, and Sane; DEF; Dvara Research; | Anupam Saraph; | No response | No response | No response | No response |
| | Bhandari, Kak, Parsheera, Rahman, and Sane; | Consent should be the fundamental ground for the collection, use and disclosure of personal data. However, the law should recognise other permitted grounds such as lawful requirements and legitimate business purposes. Consent | No response | As consent and notice cannot be treated as the sole or primary mechanism for ensuring privacy protections, the law should provide for the following principles:-<br>1. Principle of "privacy by | No response |

| | | | | | |
|---|---|---|---|---|---|
| EFF; EPIC; IFF; Omidyar Network; Privacy International Subhasis Banerjee; Suyash Rai; The Hoot. | | should be obtained in an informed and meaningful manner. There should be distinction between the different stages of data processing so that data controllers and processors can identify the appropriate standards of consent and the permissible alternatives to consent for every different stage. | | design" – It implies that privacy requirements should be taken into account at every stage of the design of a new system.<br>2. Privacy notices must be provided in a form and manner that is suitable for the requirements of the data subject to provide their meaningful and informed consent. | |
| | DEF | No response | No response | No response | No response |
| | Dvara Research | Even if consent is an important part of data collection regime, it shouldn't be a primary ground for collection and processing of personal data. The test for legitimate interest | Consent should be received from a person with parental responsibility for the child, whose personal data is being collected. | The law should mandate that entities collecting data should provide privacy notice comprising the following information:<br>1. Name and contact | A test of "Legitimate purpose" should be the primary grounds for processing data in each stage of the data life-cycle. Under this approach, personal data would only be collected, |

| | | | | | |
|---|---|---|---|---|---|
| | | should be the primary grounds for processing data. | | information of the data controller or its representative;<br>2. Voluntary or mandatory nature of data collection and associated consequences;<br>3. Contact for revoking consent;<br>4. Purpose for which data is being collected;<br>5. Details of personal data collected from third parties;<br>6. Information related to whom the data may be disclosed to;<br>7. Description of right to access/withdraw shared personal data; | processed, shared or retained. The test requires personal data use to be lawful, necessary for the provision of the good or service, and proportionate i.e. balanced against the rights of the individual. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | 8. Information regarding any form of automated data processing that may be carried out. | |
| | EFF | No response | No response | No response | No response |
| | EPIC | No response | No response | No response | No response |
| | IFF | Concern was expressed against the deployment of technology frameworks (or, "consent stacks") for consent or privacy protections that undermines consent, purpose limitations and accountability. | No response | No response | No response |
| | Omidyar Network | Informed and meaningful consent should be the primary ground for processing data. User control should be the bedrock of a data protection regime. Consent should be unambiguous, well- | No response | Notice is the minimum requirement for any kind of data processing. It must be available in non-consent grounds for data processing. | No response |

| | | | | | |
|---|---|---|---|---|---|
| | | informed, clearly articulated, specific, time-bound, revocable and auditable. | | | |
| | Privacy International | Consent shouldn't be used as a means to disclaim liability for processing. Consent should be meaningful it is accompanied by effective safeguards. Consent must be freely given, informed and specific to the processing in question. Before consent is obtained, the individuals should be informed in a clear, accessible and intelligible way about the processing and what they are consenting to. Consents should not be presented as a take it or leave it option. For consent to be freely given, individuals should be able to withdraw consent in the future. | No response | Notice should be provided to the data subject both when the data is collected from the data subject and from a third party. Privacy or data protection impact assessments can evaluate the effectiveness of notice. Enforcement and redress mechanisms must also be available to ensure that data controllers take their notice obligations seriously. The form of notices will be context specific however data protection law should contain prescriptive provisions as to what information, as a minimum, a privacy notice should contain. | |

| | | | | | |
|---|---|---|---|---|---|
| | Subhasis Banerjee | Informed consent and notice has been considered as foundational principles for privacy protection however consent and notice are usually ineffective because of information overload, limited choice and consent fatigue. Combination of legitimate interest and purpose limitation should be adopted under the regulatory control required for privacy protection. | No response | No response | It is suggested that legitimate interest and purpose limitation should be adopted as other grounds necessary for privacy protection. |
| | Suyash Rai | Regulation of "informed consent" will require complex assessments to determine if the consent was truly informed and meaningful. However achieving "informed consent" should be the main purpose of the proposed law. | No response | No response | No response |

| | | | | | |
|---|---|---|---|---|---|
| | The Hoot | No response | No response | No response | No response |

*__Industry Associations:__ ITI – Information Technology Industry Council, BSA – Business Software Alliance, iSPIRT – Indian Software Product Industry Round Table.

**__Civil Society Organisations:__ Access Now; CCG – Centre for Communication Governance, NLU Delhi; CIS – The Centre for Internet and Society; Dr. James J. Nedumpara and Mr. Sandeep Thomas Chandy, Centre for Trade and Investment Law, Ministry of Commerce; Harvard FXB Center – Harvard FXB Center for Health and Human Rights; IDP – Internet Democracy Project; Mozilla Foundation; ORF – Observer Research Foundation; Professor Graham Greenleaf; SFLC – Software Freedom Law Centre; Legal Academics and Advocates – Submission by 24 Legal Academics and Advocates, and Takshashila Institution.

***__Others:__ Anupam Saraph; Vrinda Bhandari- Advocate, Amba Kak- Mozilla Foundation, Smriti Parsheera, Faiza Rahman, and Renuka Sane- National Institute of Public Finance and Policy; DEF- Digital Empowerment Foundation; Dvara Research; EFF- Electronic Frontier Foundation; EPIC- Electronic Privacy Information Centre; IFF- Internet Freedom Foundation; Subhashish Bhadra, Associate, Omidyar Network; Privacy International; Subhasis Banerjee- Computer Science and Engineering, IIT Delhi; Suyash Rai- Senior Consultant, National Institute of Public Finance and Policy; The Hoot..